Cyclic codes: review

- A *cyclic code* is a LBC such that every cyclic shift of a codeword is a codeword.
- A cyclic code has *generator polynomial* $g(x)$ that is a divisor of every codeword.
- The generator polynomial is a divisor of $x^n - 1$, where n is blocklength.
- The parity-check polynomial is $h(x) = \dfrac{x^n - 1}{g(x)}$.
- Codewords can be generated by:

$$\begin{aligned} \text{nonsystematic:}\quad & m(x) \to m(x)g(x) \\ \text{systematic:}\quad & m(x) \to x^{n-k}m(x) - R_{g(x)}\big(x^{n-k}m(x)\big) \end{aligned}$$

- Codewords can be characterized by (and errors detected by):

$$c(x) \bmod g(x) = 0$$
$$c(x)h(x) = 0 \bmod (x^n - 1)$$

Examples of binary cyclic codes

Example: Over $\mathrm{GF}(2)$ the cyclic polynomial of degree 6 can be factored as

$$x^6 - 1 = (x^3 \pm 1)^2 = (x+1)^2(x^2+x+1)^2 \,.$$

The binary cyclic codes of blocklength 6 have generator polynomials

$$(x+1)^i(x^2+x+1)^j \,, \quad 0 \le i \le 2 \,,\ 0 \le j \le 2$$

None of these 9 cyclic codes is interesting — poor minimum distance.

Example: Over $\mathrm{GF}(2)$, $x^7 - 1 = (x+1)(x^3+x+1)(x^3+x^2+1)$.

There are $2^3 = 8$ divisors $x^7 - 1$ and thus 8 cyclic codes of blocklength 7.

Primitive polynomial yields *cyclic* Hamming code; e.g., $g(x) = x^3 + x + 1$.

$$G = \left[\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \implies H = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$$

The "dual" code has generator matrix H, the $(7,3)$ *maximum-length code*. All nonzero codewords have the same weight, $2^{m-1} = 4$.

Cyclic codes of blocklength 15

Over $\mathrm{GF}(2)$ the cyclic polynomial $x^{15}-1$ has five distinct prime factors:

$$x^{15}-1 = (x+1)(x^2+x+1)\cdot (x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

There are 2^5 cyclic codes. Some of the more useful generator polynomials:

(x^4+x+1)	(15,11) binary cyclic Hamming
$(x^4+x+1)(x^4+x^3+x^2+x+1)$	(15,7) 2-error-correcting BCH
$(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)$	(15,5) 3EC BCH
$(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x+1)$	(15,4) maximum-length

These codes, with $d^* = 3,\ 5,\ 7,\ 8$, are obtained by expurgation.

Weight	1	0	0	35	105	168	280	435	435	280	168	105	35	0	0	1
distributions of	1	0	0	0	0	18	30	15	15	30	18	0	0	0	0	1
blocklength 15	1	0	0	0	0	0	0	15	15	0	0	0	0	0	0	1
cyclic codes	1	0	0	0	0	0	0	0	15	0	0	0	0	0	0	0

Equivalent codes

The cyclic $(7,4)$ Hamming code is different from earlier $(7,4)$ Hamming code; check bits are in positions $1,2,3$ instead of $1,2,4$.

$$H_{\text{old}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \neq H_{\text{cyclic}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Definition: Two block codes that are the same except for a permutation of the symbol positions are called *equivalent*.

- Equivalent codes have same weight distribution and minimum weight.
- Not every linear block code is systematic. Consider this generator matrix:

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

- Every linear block code is equivalent to a linear block code that has a systematic generator matrix $G = [\,P \mid I\,]$ (or $G = [\,I \mid P\,]$).

Parity-check polynomial

The *parity-check polynomial* of cyclic code with generator polynomial $g(x)$ is

$$h(x) = \frac{x^n - 1}{g(x)}\,.$$

The degree of the parity-check polynomial is $n - (n-k) = k$.
Parity-check polynomial defines a relation satisfied by all codewords:

$$\begin{aligned} c(x)h(x) &= m(x)g(x)h(x) \;=\; m(x)(x^n - 1) \\ &= x^n m(x) \;-\; m(x) \;=\; 0 \bmod (x^n - 1) \\ &= (0,\ldots,0,m_0,\ldots,m_{k-1}) - (m_0,\ldots,m_{k-1},0,\ldots,0) \end{aligned}$$

Therefore coefficients of x^i in $c(x)h(x)$ are 0 for $i = k,\ldots,n-1$.
This corresponds to $n - k$ check equations:

$$\begin{array}{lcl} x^k & \Longrightarrow & 0 = c_0 h_k + c_1 h_{k-1} + \cdots + c_{k-1} h_1 + c_k h_0 \\ x^{k+1} & \Longrightarrow & 0 = c_1 h_k + c_2 h_{k-1} + \cdots + c_k h_1 + c_{k+1} h_0 \\ \vdots & & \qquad\qquad\qquad\qquad \vdots \\ x^{n-1} & \Longrightarrow & 0 = c_{n-k-1} h_k + c_{n-k} h_{k-1} + \cdots + c_{n-2} h_1 + c_{n-1} h_0 \end{array}$$

Parity-check matrix: nonsystematic

The $n - k$ check equations obtained from $c(x)h(x) = 0 \bmod (x^n - 1)$ correspond to a *nonsystematic* parity-check matrix:

$$H_1 = \begin{array}{c} \begin{array}{ccccccccc} c_0 & c_1 & \cdots & c_{k-1} & c_k & c_{k+1} & c_{k+2} & \cdots & c_{n-1} \end{array} \\ \begin{bmatrix} h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 \\ 0 & \cdots & 0 & 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 \end{bmatrix} \end{array} = \begin{bmatrix} h^R(x) \\ x h^R(x) \\ \vdots \\ x^{n-k-2} h^R(x) \\ x^{n-k-1} h^R(x) \end{bmatrix}$$

This matrix has the same form as the nonsystematic generator matrix.

The rows of H_1 are shifts of the *reverse* of $h(x)$.

$$h^R(x) = h_k + h_{k-1}x + \cdots + h_1 x^{k-1} + h_0 x^k \,.$$

Since $h(x)$ is also a divisor of $x^n - 1$, it generates an $(n, n-k)$ cyclic code.

Parity-check matrix: nonsystematic (cont.)

Since $h^R(x) = x^k h(x^{-1})$, zeroes of $h^R(x)$ are reciprocals of zeroes of $h(x)$. Thus $h^R(x)$ is also called the *reciprocal polynomial*.

The equation

$$\begin{aligned} g^R(x)h^R(x) &= (g(x)h(x))^R \\ &= (x^n - 1)^R \;=\; 1 - x^n \;=\; -(x^n - 1) \end{aligned}$$

shows that $h^R(x)$ is a divisor of $x^n - 1$.

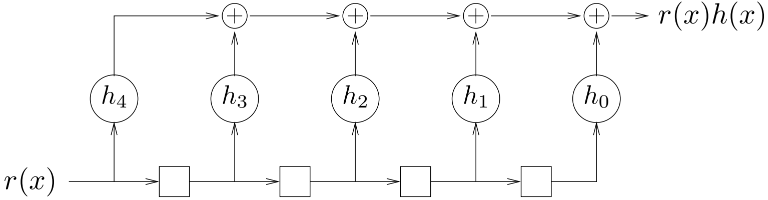
Parity-check matrix H_1 has the form of a nonsystematic generator matrix.

Rows of H_1 are shifts of the reversal polynomial $h^R(x)$. Thus $h_0^{-1}h^R(x)$ generates a cyclic code.

The cyclic code generated by $h(x)$ consists of the *reversals* of the dual of the cyclic code generated by $g(x)$.

Syndrome circuit #1

Syndrome computation circuit corresponding to H_1 multiplies by the fixed polynomial $h(x)$.



This circuit convolves input sequence $r_0, r_1, \ldots, r_{n-1}$ with parity-check polynomial coefficient sequence $h_0, h_1, \ldots, h_k$.

Since $\deg r(x) \leq n-1$, the product $r(x)h(x)$ has degree $\leq n-1+k$.

Only $n-k$ of the $n+k$ coefficients of $r(x)h(x)$ are used as the syndrome.

The syndrome consists of the coefficients of $x^k, \ldots, x^{n-1}$ in $r(x)h(x)$.

These are generated after $r_{n-1}, \ldots, r_{n-k}$ have been shifted into the register.

Syndrome polynomial

We can obtain the systematic parity-check matrix from the systematic generator matrix using the general approach:

$$G = [\,P \,|\, I\,] \implies H = [\,I \,|\, -P^T\,]$$

Direct construction: define *syndrome polynomial* to be the remainder of division by generator polynomial:

$$s(x) \;=\; r(x) \bmod g(x) \;=\; s_0 + s_1 x + \cdots + s_{n-k-1} x^{n-k-1}$$

Every codeword is a multiple of $g(x)$, so codewords have syndrome 0. Thus

$$\begin{aligned} s(x) = r(x) \bmod g(x) \;&=\; (c(x) + e(x)) \bmod g(x) \\ = c(x) \bmod g(x) + e(x) \bmod g(x) \;&=\; e(x) \bmod g(x) \end{aligned}$$

The remainder function is linear in the dividend $r(x)$.

Therefore remainders of all n-tuples are linear combinations of

$$x^i \bmod g(x) \qquad (i = 0, 1, \ldots, n-1)$$

Parity-check matrix: systematic

Polynomial syndrome $s(x)$ corresponds to systematic parity-check matrix:

$$H_2 = \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{n-k-1} \\ x^{n-k} \bmod g(x) \\ \vdots \\ x^{n-1} \bmod g(x) \end{bmatrix}^T = \begin{bmatrix} 1 & 0 & \cdots & 0 & s_0^{[n-k]} & \cdots & s_0^{[n-2]} & s_0^{[n-1]} \\ 0 & 1 & \cdots & 0 & s_1^{[n-k]} & \cdots & s_1^{[n-2]} & s_1^{[n-1]} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & s_{n-k-1}^{[n-k]} & \cdots & s_{n-k-1}^{[n-2]} & s_{n-k-1}^{[n-1]} \end{bmatrix}$$

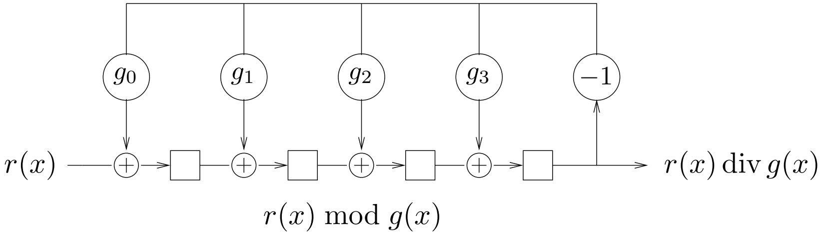
Column i of H_2 is syndrome of x^i, consists of coefficients of $x^i \bmod g(x)$.

Special case: column $n-k$ consists of coefficients of $-g(x)$ except x^{n-k}.

Column i is obtained from column $i-1$ by a linear feedback shift.

Syndrome circuit #2

Syndromes corresponding to H_2 can be calculated very efficiently using linear feedback shift register circuits that implement polynomial division.



Encoding circuits can also be used for syndrome computation:

$$\text{syndrome} = \text{actual check symbols} - \text{expected check symbols}$$

where expected check symbols are computed from received message symbols using the above encoder.

Partial syndromes

The zeroes of the generator polynomial determine codewords:

$$c(x) \text{ is codeword } \iff c(\beta) = 0 \text{ for every zero } \beta \text{ of } g(x).$$

(The "if" holds when $g(x)$ has no repeated zeroes, i.e., repeated factors.)

The zeroes of $g(x)$ belong to extension field $\mathrm{GF}(q^m)$ of $\mathrm{GF}(q)$.

Let $\{\beta_1, \ldots, \beta_t\}$ include at least one zero of each prime factor of $g(x)$.

The *partial syndromes* $S_1, \ldots, S_t$ of $r(x)$ are defined to be

$$S_i = r(\beta_i) = r_0 + r_1\beta_i + \cdots + r_{n-1}\beta_i^{n-1} \qquad (i = 1, \ldots, t)$$

The partial syndromes belong to the same extension field as $\beta_1, \ldots, \beta_t$.

Syndrome component S_i corresponds to m linear equations over $\mathrm{GF}(q)$.

The equations are linearly dependent if β_i is in a proper subfield of $\mathrm{GF}(q^m)$.

Example: cyclic Hamming code

Let $p(x)$ be a primitive polynomial over $\mathrm{GF}(2)$ of degree m.

The smallest value of n such that $p(x) \mid (x^n - 1)$ is $n = 2^m - 1$.

Cyclic code generated by $p(x)$ has blocklength $n = 2^m - 1$.

The parity-check matrix H whose columns are $x^i \bmod p(x)$ has distinct nonzero columns, so the code can correct all single errors.

The columns of H are powers of $\alpha = x$ in $\mathrm{GF}(2^m)$:

$$H \;=\; \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-2} & \alpha^{n-1} \end{bmatrix}$$

Assume a single error in location i, i.e., $e(x) = x^i$. Partial syndrome for α:

$$\begin{aligned} S_1 &= r(\alpha) = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} \\ &= c(\alpha) + e(\alpha) \;=\; e(\alpha) \;=\; \alpha^i\,. \end{aligned}$$

Decoder must find error location i from syndrome $S_1 = \alpha^i$, i.e., decoder must compute a discrete logarithm base α.

Nonbinary Hamming codes

Every 1EC code has $d^* \geq 3$, hence any two columns of check matrix are LI, hence no column of H is a multiple of another column.

There are $q^m - 1$ m-tuples over $\mathrm{GF}(q)$. The largest number of pairwise LI columns is

$$\frac{q^m - 1}{q - 1} = q^{m-1} + q^{m-2} + \cdots + q + 1\,.$$

since we can use only one of the $q - 1$ nonzero multiples of any m-tuple.

We normalize columns by requiring first nonzero entry to be 1. Example:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 \end{bmatrix}.$$

Decoding procedure for this $(13, 10)$ code:

1. Compute syndrome $s = rH^T$.
2. Normalize syndrome by dividing by first nonzero entry s_i.
3. Equal column of H is error location, and s_i is error magnitude.

Cyclic nonbinary Hamming codes

A cyclic nonbinary Hamming code is defined by an element β of $\mathrm{GF}(q^m)$ of order $n = (q^m - 1)/(q - 1)$. The check matrix is

$$H = \begin{bmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{n-1} \end{bmatrix},$$

and $g(x)$ is the minimal polynomial over $\mathrm{GF}(q)$ of β. (Fact: $\deg g(x) = m$)

Columns of H are LI over $\mathrm{GF}(q)$ if and only if $\beta^j/\beta^i = \beta^l$ is *not* in $\mathrm{GF}(q)$.

Fact: There exists a cyclic Hamming code of blocklength n if and only if n and $q - 1$ are coprime, which is true if and only if m and $q - 1$ are coprime.

Example: If $q = 3$ then $q - 1 = 2$, so odd values of m are required.

Let $\mathrm{GF}(3^3)$ be defined by primitive polynomial $x^3 + 2x + 1$, and $\beta = \alpha^2$.

$$H = \begin{bmatrix} 1 & \alpha^2 & \ldots & \alpha^{22} & \alpha^{24} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 0 & 2 & 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 0 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 2 \\ 0 & 1 & 1 & 1 & 2 & 1 & 1 & 0 & 0 & 1 & 2 & 0 & 2 \end{bmatrix}.$$

The generator polynomial $x^3 + x^2 + x + 2$ can be found by several methods, then used to construct a systematic parity-check matrix.

Cyclic binary Golay code

Multiplicative orders of elements of $\mathrm{GF}(2^{11})$ divide $2^{11} - 1 = 23 \cdot 89$.

There are $\phi(23) = 22$ elements of order 23. Conjugates of any such β are

$$\beta,\ \beta^2,\ \beta^4,\ \beta^8,\ \beta^{16},\ \beta^9,\ \beta^{18},\ \beta^{13},\ \beta^3,\ \beta^6, \beta^{12}$$

The minimal polynomial has degree 11. Prime polynomials of degree 11 are

$$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$$
$$\tilde{g}(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

These polynomials are mirror images; their zeroes are reciprocals.

Consecutive powers $\beta, \beta^2, \beta^3, \beta^4$ among the conjugates guarantee $d^* \geq 5$.

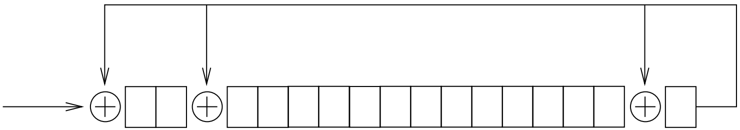
Lemma: Golay codewords of even weight have weight a multiple of 4.

Theorem: The cyclic Golay codes has $d^* = 7$ and in fact are perfect codes.

Weight enumerator: $1 + 253x^7 + 506x^8 + 1288x^{11} + 1288x^{12} + 506x^{15} + 253x^{16} + x^{23}$

Examples of cyclic codes: CRC-16

Cyclic codes are often used for error detection because the encoding and syndrome calculation circuits are *very* simple.



The most common generator polynomial is CRC-16:

$$\text{CRC-16} \;=\; x^{16} + x^{15} + x^2 + 1 \;=\; (x+1)(x^{15} + x + 1)$$

CRC-16 is simplest polynomial of degree 16 with degree 15 primitive factor. The factor $x^{15} + x + 1$ is primitive of degree 15 hence has order $2^{15} - 1$.

Therefore the *design* blocklength of CRC-16 is $2^{15} - 1 = 32767$ bits.

A significantly shortened code is almost always used.

Examples of cyclic codes: CRC-CCITT

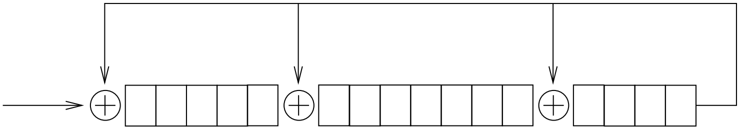
Another popular generator polynomial is

$$< \text{CRC-CCITT} \;=\; x^{16} + x^{12} + x^5 + 1 \;=\; (x+1)p_2(x)\,,$$

where $p_2(x)$ is a primitive polynomial of degree 15:

$$p_2(x) = x^{15} + x^{14} + x^{13} + x^{12} + x^4 + x^3 + x^2 + x + 1$$

CRC-16 and CRC-CCITTT polynomials have only 4 nonzero coefficients, so the shift register coding circuits need only 3 exclusive-or gates.



Minimum distance for CRC-16, CRC-CCITT is 4. Both codes correct single errors while detecting double errors, or detect up to 3 errors.

Any cyclic code with $n - k = 16$ detects burst errors of length 16 bits, which is optimal.